2013

Sellers Continue to Give Away Confidential Information on Second Hand Memory Cards Sold in Australia

Patryk Szewczyk
Edith Cowan University, p.szewczyk@ecu.edu.au

Nikki Robins
Edith Cowan University

Krishnun Sansurooah
Edith Cowan University, k.sansurooah@ecu.edu.au

DOI: 10.4225/75/57b3dac1fb876
11th Australian Digital Forensics Conference. Held on the 2nd-4th December, 2013 at Edith Cowan University, Perth, Western Australia

SELLERS CONTINUE TO GIVE AWAY CONFIDENTIAL INFORMATION ON SECOND HAND MEMORY CARDS SOLD IN AUSTRALIA

Patryk Szewczyk[1, 2], Nikki Robins[1], Krishnun Sansurooah[1, 2]
School of Computer and Security Science, Edith Cowan University[1]
Security Research Institute, Edith Cowan University[2]
Perth, Australia

Abstract
Second hand storage devices can be treasure troves of confidential data. This study investigated the remnant data on second hand memory cards that were purchased through Australian second hand auction websites throughout 2013. Memory cards continue to increase in capacity and are used in both smart phones and tablet computers as persistent storage. During this study a total of 140 second hand memory cards were purchased throughout 2013. Each memory card had its data recovered and subsequently analysed. The results show that sellers are sending memory cards with no evidence of erasure; poor attempts to erase data; or simply asking the buyer to erase the data prior to use. The data recovered is not only of a personal nature, but also appears to originate from Australian government departments and business. It is evident that actions must be taken by second hand auction sites, and the media to raise awareness and educate end-users on how to dispose of data in an appropriate manner.

Keywords
Digital forensics, memory cards, flash memory, remnant data, eBay, auction

INTRODUCTION

Remnant data on persistent storage devices has been a prominent, issue for many years. Regardless of whether the data was recovered from a hard disk drive (Valli & Woodward, 2008), USB flash drive (Chaerani, Clarke, & Bolan, 2011) or memory card (Szewczyk & Sansurooah, 2012), confidential data is consistently present. Memory cards are inexpensive, versatile and used in a vast array of consumer electronic devices. Vendors typically limit the in-built storage capacity of electronic devices, and subsequently permit end-users to increase or replace the device's storage capacity through the use of a memory card.

Memory cards are widely used in a large variety of consumer electronic devices, but have been a predominant component of smart phones and tablet computers in recent years. Previous research has shown that memory cards like USB flash drives and hard disk drives may contain a significant quantity of confidential data (Szewczyk & Sansurooah, 2011, 2012). Further adding to the dilemma is that the data is not only of a personal nature, but also appears to originate from Australian commercial or Government entities. This raises a concern over the effectiveness of corporate policies and controls which restrict or limit sensitive data being removed from a company's premises.

Many of today's electronic devices such as smart phones and tablet computers are small and portable. As a result, end-users are increasingly using their portable electronic devices at work, and accessing and storing confidential company data. The confidential data may have been stored on the smart phone or tablet computer and may subsequently leave the company. This is an unfortunate outcome of employers permitting a Bring Your Own Device (BYOD) model. However, with employees following a BYOD model this raises future legal issues as companies are increasingly losing control of confidential data (Kennedy, 2013). Clients and customers of corporations using a BYOD model may have a genuine concern regarding the confidentiality of data and where it may end up.

The research into investigating whether or not remnant data on memory cards is in fact a genuine issue has been proven through prior research (Szewczyk & Sansurooah, 2011, 2012). Data that remains on second hand memory cards in order of occurrence typically includes multimedia files,

photos, private personal documents, sexualised images, and Government or commercial files. The prior research has shown that there is often sufficient private personal data to commit identity fraud, or alternative forms of cyber attacks. In addition, there is a significant issue with the quantity of memory cards that are adequately wiped – to ensure that data is unrecoverable. In 2011, twelve percent of memory cards were not recoverable with this figure increasing to twenty-nine percent in 2012. Despite the significant increase, there was also an increase in the quality of the data recovered – in terms of how confidential and sensitive the data would be to a person or organisation. End-users may genuinely perceive there to be little threat with selling second hand memory cards, thus this third iteration re-investigates if the issue of disposing of confidential information remains a growing concern.

RESEARCH PROCEDURE

Between November 2012 and October 2013, 140 second hand memory cards were procured and analysed. The memory cards were all purchased through the second hand auction site eBay – Australia. The memory cards were located on eBay through the mobile phone and camera categories. Only memory cards deemed used or refurbished by the seller were purchased outright or bid on. This study had been conducted previously and thus certain sellers were avoided. Specifically sellers who appeared to operate an online business and who had previously sold a memory card which did not contain any data of interest were not purchased.

Prior research and an informal survey of electronics devices concluded that microSD and standard SD cards were the prominent form of persistent storage utilised in consumer based electronic devices. Subsequently, the plan was to focus predominantly on the purchase of the aforementioned memory cards. However, as the study had progressed over the course of the year, the researchers identified that the alternative forms of second hand memory cards were not being regularly sold through eBay.

Table 1 Comparison of memory card types purchased

Memory Card Type	Quantity in 2011	Quantity in 2012	Quantity in 2013
microSD card	64 (55%)	45 (58%)	91 (65%)
miniSD card	4 (3%)	0	0
SD card	13 (11%)	26 (33%)	49 (35%)
Memory Stick Pro Duo	8 (6%)	2 (3%)	0
M2 card	18 (15%)	2 (3%)	0
Compact Flash	12 (10%)	2 (3%)	0

To ensure that sellers are not prompted to take additional measures to erase data from memory cards, multiple aliases of the researchers involved were utilised to purchase memory cards. The quantity and capacity of memory cards being sold through eBay in 2013 was significantly higher than in previous years. Whilst there was a significant quantity of memory cards for sale, there appeared to be a high demand for the memory cards also. This could have been a direct result of consumers wishing to upgrade the storage capacity of their electronic devices. In 2011, approximately ninety-six percent of all memory cards listed were purchased by the researchers. In 2012 this figure dropped to approximately seventy-one percent. In 2013, less than forty percent of second hand memory cards available on eBay – Australia were procured by the researchers. Quantity of cards purchased was monitored through daily eBay notifications which would detail any new listing within the last twenty-four hour period.

Table 2 Quantity and capacity of memory cards purchased

Size of Memory Card	Quantity in 2011	Quantity in 2012	Quantity in 2013
32 MB	1 (1%)	0	
64 MB	9 (8%)	0	
128 MB	13 (11%)	2 (3%)	1 (1%)
256 MB	9 (8%)	0	1 (1%)
512 MB	19 (16%)	0	0 (0%)
1 GB	38 (32%)	17 (22%)	23 (16%)
2 GB	26 (22%)	20 (26%)	25 (18%)
4 GB	3 (3%)	14 (18%)	21 (15%)
8 GB	1 (1%)	15 (19%)	33 (24%)
16 GB	0	6 (8%)	12 (9%)
32 GB	0	3 (4%)	18 (13%)
64 GB	0	0	6 (4%)

The same method utilised to previously acquire and analyse the data from the memory cards was followed throughout this study (Szewczyk & Sansurooah, 2012). A raw dd image was created of each memory card using FTK Imager 3.1.2 (FTK Imager, 2013). Recovery and analysis was subsequently undertaken using X-Ways WinHex v17.2 (Reischmann, 2013) via the File Recovery by Type function. An analysis was also undertaken using Autopsy 3.0.4 (Carrier, 2013).

REMNANT DATA RESULTS

Despite the media issuing warnings relating to the issues of improper persistent storage disposal (DeCeglie, 2011; White, 2013), there was still a significant quantity of memory cards which were inadequately erased, encompassing confidential data. The sensitivity of data has also increased throughout 2013 with trends showing that memory cards coupled with smart phones and tablet computers are slowly replacing desktop computers. This is based on the type of data that is being stored and recovered on memory cards. Two memory cards had to be handed over to the police for further investigation of suspected illegal content. Subsequently, memory cards may slowly encompass more illegal content and may be more prominent as potential source of evidence in a court of law.

Twenty-seven percent (38) of the memory cards were not recoverable based on the tools utilised to recover data. It assumed that the seller or previous owner had taken and utilised the appropriate actions to permanently remove data from the memory card. The twenty-seven percent is slightly lower than the quantity of erased memory cards from last year which was at twenty-nine percent (Szewczyk & Sansurooah, 2012). Fifty-nine percent (82) memory cards appeared to have data removed, but could be easily recoverable using the aforementioned computer forensic tools. Unfortunately, despite prior media warnings, fourteen percent (20) memory cards showed no attempt to permanently remove the data. In these instances, once the memory card was connected to the investigating computer, all data was readily accessible. As depicted through Table 3

Table 3 Types of information recovered from all memory cards

Information Type Recovered	Quantity of Memory Cards
Photographic images	87 (62%)
Multimedia (audio, video)	58 (41%)
Private personal documentation	15 (11%)
Business cards (e.g. vCard)	11 (8%)
Pornographic material	8 (6%)
Government or business documents	8 (6%)
Online authentication credentials	7 (5%)
Resumes	3 (2%)

As in previous years, photographic images and multimedia files were prominent amongst the memory cards investigated. Overall, there were slightly less memory cards that contained private personal documentation and subsequently, the quantity of resumes (which contain a substantial wealth of data) was also less. There were twenty-one notable cases amongst the lot from 2013. Six of the more significant ones have been briefly summarised below. The case numbers reflect the order of analysis, and do not reflect in anyway the purchasing order.

- Case 24 had been deleted, yet the data was recoverable. The memory card appeared to have been used in an Australian Government department as it had contained email addresses and personally identifiable information pertaining to a group of employees. The envelope in which the memory card was shipped clearly identified the organisation and reflected the employee details. A series of files appearing to be a history of SMS messages were present plus a few pornographic files.

- Case 42 had been deleted, yet the data was recoverable. The memory card may have been used in a smart phone, and contained movies and music. Various utility statements and tax invoices were present with clearly identifiable personal information. The information present on the documents clearly reflected the personal details from whom the memory card was originally purchased from.

- Case 43 had been deleted, yet the data was recoverable. The memory card contained tax related documentation and rental agreements and receipts. The owner of the card may have been a student as both assignments and enrolment documents had been recovered. A small document was also present with a couple of usernames and passwords to various online services.

- Case 47 had been deleted, yet the data was recoverable. Hundreds of holiday photos were recovered from the memory card. Amongst the photos were a couple of pictures of an application for an Australian passport with all details clearly visible. Payslips were present for the individual in the passport application as well as travel itineraries and boarding passes for a local upcoming holiday. SMS conversations were recovered that occurred between various parties, with information that could potentially embarrass the parties involved.

- Case 58 had been deleted, yet the data was recoverable. Various photos were recovered but nothing of significant interest. It appears that the individual was applying or accepting a job as a detailed resume was present, in conjunction with covering letters, signed copies of company agreements, computer account agreement forms, and banking and tax forms.

- Case 69 encompassed both deleted and non-deleted data. The memory card encompassed a significant quantity of pirated and pornographic material. One utility bill stated personal information regarding an individual. Amongst the photos on the card was a picture of an individual in their bedroom standing in front of (presumably) their awards and achievements. Their name was clearly visible on the parchment in the background. The name on the parchment reflected the name on the utility bill. One additional document was present which encompassed a long list of authentication credentials to many online services.

Sixty-two percent of memory cards encompassed photos. Many photos were sexualised with the faces of the individual clearly present. A reoccurring issue pertains to there usually being at least one other (recoverable) file on the memory card which identifies the individual in the photos. The photographic images issue is further concerning in that individuals appear to be taking photos of their own confidential documents. In some instances, the photo is taken with the device's camera, and in other instance the photo is a result of a screenshot of a website.
During the 2012 investigation (Szewczyk & Sansurooah, 2012) a number of sellers included brief notes asking the buyer to erase all data on the memory cards prior to usage. This has the potential

to encourage a buyer to snoop through the memory card's data. Unfortunately, this lazy and ignorant behaviour continued throughout 2013, with the inclusion of similar notes accompanying memory cards. One seller admitted that they were not sure if they had removed the data from the memory card appropriately, and were apologetic if data still existed. In this unique instance, the data had not been removed adequately.

The issue of sellers inadvertently encouraging buyers to snoop through data on memory cards was also evident in the manner that item was being listed eBay. Two sellers stated in their listing that the memory cards being sold had not been erased due to time constraints, and are being sold *as is*. Time constraints may be a genuine factor in not permanently erasing data from memory cards. However, the awareness and education factor is presumably the larger issue. Individuals may genuinely be unaware of the appropriate procedure for wiping data, lack the appropriate tools to do so, and are unaware of the dangers of leaving data intact. Familiarity of tools may also be an issue. End-users who are only coming to terms with being able to use desktop data wiping tools, may lack the knowledge and expertise to apply these same tools and procedure to a storage medium typically only used in smart phones or tablet computers.

Based on the three re-iterations of this research it is anticipated that this issue will remain constant. Apple iPad products do not encompass facilities to permit consumers to increase their storage capacity via a memory card. In contrast, not only are Android and Microsoft based products outselling and dominating the smart phone and tablet market (Golson, 2013; Kleinman, 2013), but they also encompass means to enable consumers to change and upgrade the storage capacity via a memory card. The prevalence of confidential information being stored on the device will gradually increase as research is showing that consumers are happy to replace their desktop or laptop computer with a tablet computer (Terrenghi, Garcia-Barrio, & Oshlyansky, 2013). In addition with more corporations utilising a BYOD model, the results suggest that more government and commercial data will be finding its way onto second hand auction sites without the seller being truly aware of what they are selling.

CONCLUSION

Inappropriate disposal of persistent storage media has been a long standing issue. It is somewhat understandable that a seller may not understand the risks, and may lack the knowledge to adequately appropriately wipe data. However, asking the buyer to wipe data is dangerous and unjustifiable behaviour. This is crucially important when the memory may contain government or corporate data. With tablet computers being adopted into hospital and medical environments, there is an increased risk of medical data finding its way onto second hand auction websites.

Second hand auction sites are at the forefront of encouraging and teaching individuals of the risks and procedures required to adequately wipe data permanently. Unfortunately, such practices are not taking place. In previous years eBay warned sellers to ensure all data is removed. It now appears that this warning is no longer present. As portrayed by this research, it is evident that more needs to happen to stop confidential data being leaked through second hand auction sites. Subsequently, eBay should provide step-by-step procedures detailing how an end-user can adequately wipe data on a hard disk drive, USB flash drive and memory cards.

This research will continue in subsequent years and will focus predominantly on the microSD and standard SD cards which are appear to be the predominant persistent storage media for smart phones and tablet computers. As the need for a desktop or laptop computer diminishes with the continual improvements to portable computing devices, it is highly likely that each memory card purchased will contain some confidential remnant data.

REFERENCES

Carrier, B. (2013). The Sleuth Kit Retrieved September 13, 2013, from http://www.sleuthkit.org/autopsy/download.php

Chaerani, W., Clarke, N., & Bolan, C. (2011). *Information leakage through second hand USB flash drives within the United Kingdom*. Paper presented at the 9th Australian Information Security Management Conference Citigate Hotel, Perth, Western Australia.

DeCeglie, A. (2011). WA study reveals private details exposed in sale of second-hand memory cards Retrieved November 3, 2012, from http://www.perthnow.com.au/news/your-secrets-exposed/story-e6frg12c-1226218988783

FTK Imager. (2013). Forensic Toolkit Imager Retrieved September 20, 2012, from http://accessdata.com/support/adownloads#FTKImager

Golson, J. (2013). Apple's Share of Tablet Market Drops on Increased Android Tablet Sales Retrieved September 13, 2013, from http://www.macrumors.com/2013/10/30/apples-share-of-tablet-market-drops-on-increased-android-tablet-sales/

Kennedy, S. (2013). Death of BYOD predicted Retrieved October 31, 2013, from http://www.theaustralian.com.au/technology/death-of-byod-predicted/story-e6frgakx-1226749813859

Kleinman, J. (2013). Report Says Android Overtakes Apple iPads in Q2 Tablet Sales Retrieved September 14, 2013, from http://www.technobuffalo.com/2013/09/30/android-overtakes-apple-ipads-in-q2-tablet-sales-report-says/

Reischmann, S. (2013). X-Ways Software Technology Retrieved July 25, 2013, from http://www.winhex.com/winhex/

Szewczyk, P., & Sansurooah, K. (2011). *A 2011 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia.* Paper presented at the 9th Australian Digital Forensics Conference, Citigate Hotel, Perth, Western Australia.

Szewczyk, P., & Sansurooah, K. (2012). *The 2012 Investigation into Remnant Data on Second Hand Memory Cards Sold in Australia*. Paper presented at the 10th Australian Digital Forensics Conference, Novotel Langley Hotel, Perth, Western Australia.

Terrenghi, L., Garcia-Barrio, L., & Oshlyansky, L. (2013). *Tablets use in emerging markets: an exploration*. Paper presented at the Proceedings of the 15th international conference on Human-computer interaction with mobile devices and services Munich, Germany.

Valli, C., & Woodward, A. (2008). *The 2008 Australian study of remnant data contained on 2nd hand hard disk: the saga continues.* Paper presented at the 6th Australian Digital Forensics Conference, Edith Cowan University, Perth, Western Australia.

White, N. (2013). Personal data recovered in USB swipes Retrieved March 2, 2013, from http://www.australasianscience.com.au/news/september-2013/personal-data-recovered-usb-swipes.html